

**POLÍTICA DE CERTIFICACIÓN**  
***CERTIFICATION POLICY (CP)***

**CERTIFICADOS DE SEDE ELECTRÓNICA**

**Versión 1.0**

## INDICE

1	INTRODUCCIÓN .....	3
1.1	Descripción general .....	3
1.2	Nombre del Documento e identificación.....	3
2	ENTIDADES PARTICIPANTES .....	4
2.1	Autoridades de Certificación (CA).....	4
2.2	Autoridad de Registro (RA).....	4
2.3	Solicitante .....	4
2.4	Suscriptor .....	4
2.5	Custodio de Claves.....	4
2.6	Tercero que confía en los certificados .....	4
3	CARACTERISTICAS DE LOS CERTIFICADOS .....	4
3.1	Periodo de validez de los certificados .....	5
3.2	Tipo de soporte.....	5
3.3	Certificados multidominio.....	5
3.4	Uso particular de los Certificados Administrativos de Sede Electrónica .....	5
3.4.1	Usos apropiados de los certificados .....	5
3.4.2	Usos no autorizados de los certificados .....	5
3.5	Tarifas .....	5
4	PROCEDIMIENTOS OPERATIVOS.....	6
4.1	Proceso de emisión de certificados .....	6
4.2	Revocación de certificados .....	8
4.3	Renovación de certificados.....	8
5	PERFIL DE LOS CERTIFICADOS .....	9
5.1	Campos comunes a los dos niveles.....	9
5.1.1	Certificado .....	9
5.1.2	Extensiones de los certificados .....	10
5.2	Nivel ALTO .....	10
5.2.1	Certificado .....	10
5.2.2	Extensiones de los certificados .....	10
5.3	Nivel MEDIO.....	10
5.3.1	Certificado .....	10
5.3.2	Extensiones de los certificados .....	11

# 1 INTRODUCCIÓN

## 1.1 DESCRIPCIÓN GENERAL

Los **Certificados de Sede Electrónica** son certificados expedidos a Administraciones Públicas, según los requisitos establecidos en la Ley 11/2007, de 23 de junio, de Accesos Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

La solicitud y emisión de los Certificados de Sede Electrónica se realiza a través de las Autoridades de Registro de Firmaprofesional.

Los Certificados de Sede Electrónica emitidos por Firmaprofesional no son certificados digitales reconocidos según la Ley 59/2003 de 19 de diciembre de firma electrónica.

Estos certificados pueden emitirse según dos niveles de aseguramiento, dependiendo del soporte en el que se cree y resida el par de claves:

- MEDIO: soporte *software*
- ALTO: soporte *hardware* criptográfico

La presente política sigue las definiciones de los niveles de aseguramiento del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009

En el presente documento se exponen las Condiciones Particulares referentes a este tipo de certificado. Esta Política de Certificación está subordinada al cumplimiento de las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

## 1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

<b>Nombre:</b>	CP Sede Electrónica
<b>Versión:</b>	1.0
<b>Descripción:</b>	Política de Certificación para Certificados de Sede Electrónica
<b>Fecha de Emisión:</b>	26/07/10
<b>OIDs</b>	1.3.6.1.4.1.13177.10.1.20.1 Nivel Alto – <i>Hardware</i> criptográfico 1.3.6.1.4.1.13177.10.1.20.2 Nivel Medio - <i>Software</i>
<b>Localización</b>	<a href="http://www.firmaprofesional.com/cps">http://www.firmaprofesional.com/cps</a>

## 2 ENTIDADES PARTICIPANTES

### 2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados Corporativos de Colegiado deben ser emitidos por la CA Subordinada “**AC Firmaprofesional - AAPP**”, que emite certificados digitales a Corporaciones Públicas.

### 2.2 AUTORIDAD DE REGISTRO (RA)

Firmaprofesional actuará directamente como Autoridades de Registro para la emisión de Certificados de Sede Electrónica. También podrá actuar como RA para la emisión de Certificados de Sede Electrónica cualquier entidad que tenga un contrato de vinculación de RA con Firmaprofesional.

### 2.3 SOLICITANTE

Podrá realizar la solicitud de un certificado de Sede Electrónica cualquier persona autorizada por su propia organización para ello.

### 2.4 SUSCRIPTOR

El suscriptor del certificado será una Administración Pública, identificada por su CIF y denominación, así como por medio de una URL.

### 2.5 CUSTODIO DE CLAVES

No se incluirá información del custodio de claves ni de ninguna persona física en los certificados emitidos bajo la presente política.

### 2.6 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los Certificados de Sede Electrónica están reconocidos por **@firma**, la Plataforma de validación y firma electrónica del Ministerio de la Presidencia.

### 3 CARACTERÍSTICAS DE LOS CERTIFICADOS

#### 3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los Certificados de Sede Electrónica tendrán un periodo de validez de 1, 2 o 3 años.

#### 3.2 TIPO DE SOPORTE

Los Certificados de Sede Electrónica se emitirán en soporte *software* (nivel MEDIO) o *hardware* (nivel ALTO)<sup>1</sup>.

#### 3.3 CERTIFICADOS MULTIDOMINIO

No se contempla la posibilidad de emitir certificados multidominio para sedes electrónicas por recomendaciones del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009.

#### 3.4 USO PARTICULAR DE LOS CERTIFICADOS ADMINISTRATIVOS DE SEDE ELECTRÓNICA

##### 3.4.1 Usos apropiados de los certificados

Los Certificados de Sede Electrónica pueden ser utilizados para autenticar la identidad de una sede electrónica, y establecer luego un canal de transmisión seguro entre la sede electrónica y el usuario del servicio.

##### 3.4.2 Usos no autorizados de los certificados

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.

No se permite el uso de este tipo de certificado para la firma electrónica de documentos.

#### 3.5 TARIFAS

El precio de los Certificados Administrativos de Sede Electrónica y las condiciones de pago de este tipo de certificados será necesario consultarlas telefónicamente o por mail con Firmaprofesional.

El pago por estos certificados podrá realizarse en efectivo o por transferencia bancaria.

<sup>1</sup> Los niveles vienen definidos en Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009

## 4 PROCEDIMIENTOS OPERATIVOS

### 4.1 PROCESO DE EMISIÓN DE CERTIFICADOS

Si la Corporación Pública ya ha firmado el contrato de prestación de servicios de certificación y su representante legal (el Órgano superior unipersonal de representación o el Órgano en quien se delegue o el Responsable de Recursos Humanos) dispone del certificado corporativo de persona física representante, este representante legal estará autorizado a emitir los certificados directamente accediendo a los servicios de Firmaprofesional, tramitando las correspondientes hojas de entrega.

Si la Corporación Pública no tuviera firmado el contrato de prestación de servicios de certificación con Firmaprofesional, deberá ser firmado por el representante legal en el momento de solicitar un certificado.

La corporación o una RA de Firmaprofesional se encargará de tramitar las solicitudes y proceder a la emisión de los certificados cumpliendo siempre con los términos generales descritos en la CPS.

Los pasos a seguir para la obtención del certificado se detallan a continuación:

#### a) Solicitud

Deberá ser realizada por el solicitante, cumpliendo con lo descrito en la CPS y presentando, como mínimo, la documentación siguiente:

- Cuando la tramitación la realiza directamente la Corporación Pública convertida en RA:
  - Una hoja de pedido firmada por el solicitante
  - La titularidad del nombre de dominio, certificada por un Órgano de representación de la Administración.
- Cuando la tramitación la realiza una RA que no sea la misma Corporación Pública:
  - Una hoja de pedido firmada por el solicitante y autorizada por el representante legal de la Corporación Pública
  - La acreditación por un medio fehaciente de la existencia de la entidad conforme a Derecho
  - La resolución de la Subsecretaria del Ministerio o titular del organismo público competente. La referencia al diario oficial en el que aparece la disposición de creación de la Sede Electrónica.
    - En el caso de la Administración General del Estado (AGE) este diario oficial es el BOE<sup>2</sup>.
    - Para otras Administraciones Públicas, el diario oficial correspondiente (p.e. El Diari Oficial de la Generalitat de Catalunya, el Boletín Oficial de la Diputació correspondiente, etc...
  - En caso de solicitar nivel ALTO, se deberá aportar evidencia de que la generación y custodia de claves se realiza en un dispositivo *hardware* criptográfico.

<sup>2</sup> Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (RD-LAECSP). Art. 3.2

**b) Aceptación de la solicitud**

- **Cuando la Corporación Pública es RA. La aceptación es automática ya que la RA es la misma Corporación**
- **Cuando se utiliza a Firmaprofesional o un agente comercial como RA.**, la RA verificará la aparición de la disposición de creación de la Sede en el Diario Oficial Correspondiente.

Para solicitudes de entidades pertenecientes a la AGE, validar que la dirección electrónica incluye el dominio de segundo nivel "gob.es"<sup>3</sup> y que la disposición de creación en el BOE correspondiente contiene al menos la siguiente información:

- a) **Ámbito de aplicación de la sede**, que podrá ser la totalidad del Ministerio u organismo público, o uno o varios de sus órganos con rango, al menos, de dirección general
- b) **Identificación de la dirección electrónica de referencia de la sede.**
- c) **Identificación de su titular**, así como del órgano u órganos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos en la misma.
- d) **Identificación de los canales de acceso a los servicios disponibles en la sede**, con expresión, en su caso, de los teléfonos y oficinas a través de los cuales también puede accederse a los mismos.
- e) **Medios disponibles para la formulación de sugerencias y quejas.**

**c) Tramitación**

Una vez aceptada la solicitud, la Organización pública o la RA tramitará la solicitud del certificado

**d) Generación de claves**

Las claves de firma serán generadas en los sistemas del solicitante utilizando sus propias aplicaciones compatibles con los estándares de PKI.

En caso de solicitar nivel ALTO, la generación y custodia de claves se realizará en un dispositivo *hardware* criptográfico.

El solicitante entregará a la RA una petición de certificado en formato PKCS#10.

Generalmente, las aplicaciones de servidores que pueden configurarse con el protocolo SSL, como IIS de Microsoft, incluyen herramientas para generar claves y peticiones de certificados.

<sup>3</sup>

RD-LAECSP. Art. 17.2

#### e) Emisión del certificado

La RA procederá a la emisión del certificado, firmando la petición de certificado en formato PKCS#10 y enviándola a la CA.

Una vez que se haya generado el certificado, y antes que la RA pueda entregarlo al suscriptor, éste último deberá:

- Identificarse presencialmente ante la RA, según el procedimiento que ésta le comunique.
- Recibir la Hoja de entrega y aceptación.

#### f) Entrega

Finalmente, la RA hará entrega del certificado al suscriptor permitiendo su descarga de forma segura desde Internet

## 4.2 REVOCACIÓN DE CERTIFICADOS

El suscriptor deberá solicitar la revocación de su certificado en caso de pérdida, compromiso de claves u otras causas descritas en la CPS.

Para solicitar la revocación del certificado el suscriptor puede:

1. En horario de oficina:
  - Ponerse en contacto telefónicamente o presencialmente con su RA.
2. Fuera de horario de oficina:
  - Revocar online su certificado en la página web de Firmaprofesional.
  - Llamar al servicio de revocación 24x7: 902.361.639

Para toda información complementaria referente a la revocación de los certificados, referirse al apartado correspondiente de la CPS.

## 4.3 RENOVACIÓN DE CERTIFICADOS

Existen dos procedimientos:

- a) **Proceso de renovación presencial:** El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.
- b) **Proceso de renovación online:** Si la RA dispone del servicio y el suscriptor ha contratado la renovación, éste recibirá una notificación de la RA por correo electrónico para iniciar la renovación a través de la página web de Firmaprofesional.

## 5 PERFIL DE LOS CERTIFICADOS

Los Certificados Administrativos de Sede Electrónica de Firmaprofesional siguen las recomendaciones del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009.

### 5.1 CAMPOS COMUNES A LOS DOS NIVELES

#### 5.1.1 Certificado

El DN de los Certificados Administrativos de Sede Electrónica contendrá como mínimo los elementos que se citan con el formato siguiente. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	<i>Denominación de nombre de dominio (DNS o IP) donde residirá el certificado</i>
O, Organization	Organización	<i>Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (</i>
OU, Organization Unit	Unidad en la organización	<i>"sede electrónica"</i>
OU, Organization Unit	Unidad en la organización	<i>El nombre descriptivo de la sede</i>
SN, Serial Number	Número de serie	<i>Contendrá el NIF de la entidad responsable de la sede electrónica</i>
C, Country	País	<i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i>

## 5.1.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Autenticación TSL web Server
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> <URI de la CPS>
Qualified Certificate Statements	Sí	qcCompliance qcEuRetentionPeriod: 15 años

## 5.2 NIVEL ALTO

### 5.2.1 Certificado

Campo	Nombre	Descripción
Signature Algorithm	Algoritmo de firma	RsaWithSHA1, con longitud de claves de 2048 o superior

### 5.2.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	User Notice: "Certificado reconocido de sede electrónica, nivel alto. Consulte las condiciones de uso en " + URL de la DPC
Qualified Certificate Statements	Sí	qcSSCD
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.1.1.1 = "sede electrónica" OID: 2.16.724.1.3.5.1.1.2 = <O del DN> OID: 2.16.724.1.3.5.1.1.3 = <serialNumber del DN> OID: 2.16.724.1.3.5.1.1.4 = <segundo OU del DN> OID: 2.16.724.1.3.5.1.1.5 = <CN del DN>

## 5.3 NIVEL MEDIO

### 5.3.1 Certificado

Campo	Nombre	Descripción
Signature Algorithm	Algoritmo de firma	RsaWithSHA1, con longitud de claves de 1024 o superior

### 5.3.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	User Notice: "Certificado reconocido de sede electrónica, nivel medio. Consulte las condiciones de uso en " + URL de la DPC
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.1.2.1 = "sede electrónica" OID: 2.16.724.1.3.5.1.2.2 = <O del DN> OID: 2.16.724.1.3.5.1.2.3 = <serialNumber del DN> OID: 2.16.724.1.3.5.1.2.4 = <segundo OU del DN> OID: 2.16.724.1.3.5.1.2.5 = <CN del DN>